UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/837,283	04/18/2001	Paul H. Feinberg	SONY 3.0-029	9632

530 7590 10/21/2004

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 10/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/837,283	FEINBERG, PAUL H.	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/18/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 8-16, 23-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Takagi et al (US 5,109,152).

a. *Referring to claim 8:*

i. Takagi teaches:

(1) receiving a first value from the device, the first value being different from an identifier associated with the device; determining the identifier from the value, the value being a function of the identifier and the number of times the device has been authenticated; comparing the identifier determined from the value against a pre-stored identifier; authenticating the device based on the result of the comparison **[i.e., the procedure of creating the identifier described above in connection with Figure 6 is completely identical to the procedure of data encryption shown in Figure 5, and it is possible to have the identifier creation process and data encryption process concurrently. Namely, the output of the encryption processes 223-226 in Figure 6 is sent to the second device 202 as an output (encrypted output of transmission data) of the encryption means 204. Specifically, the output of the encryption process 226, i.e., the identifier 231, in Figure 6 is the output of the encryption means 204 for the fixed pattern (P) 215 in Figure 5, and it is stored in the second register 208. Next, the second device 202 uses the second encryption means 211 which performs the same operation as of the first encryption means 204, third register 212 and third exclusive-OR operation means 213 to create comparison data in the same procedure as that of**

the first device 201 for creating the identifier 231. The comparison data is stored in the third register 212. Finally, the second device 202 uses the comparison means 214 to compare the identifier 231 stored in the second register 208 with the comparison data stored in the third register 212 thereby to verify whether or not the communication data has been tampered (column 12, line 59 through column 13, line 40). In addition, Similarly, in the second comparison means 156, the result of comparison between the random number data S.sub.2 which is inferred to have been produced by the transaction IC card 150 and the random number data S.sub.0 which has been actually generated by the second random number generation means 151 becomes a second control signal C.sub.2 for the second processing means 160, and only if both data match, it grants the second processing means 160 to have the information exchange (column 10, lines 31-40)].

b. *Referring to claims 9-14:*

i. These claims have limitations that is similar to those of claim 8, thus they are rejected with the same rationale applied against claim 8 above.

c. *Referring to claim 15:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

d. *Referring to claim16:*

i. Takagi further teaches:

(1) wherein the function is intended to make it difficult to predict the next value to be received **[i.e., (1) the identifier is dependent on all bits of data of the plain text block. (2) For a plain text m, identifier creation means f, and identifier a=f(m), it is very difficult to obtain x which meets the following: f(m)=f(x) (column12, lines 51-57)].**

e. *Referring to claim 23:*

i. Takagi teaches:

(1) maintaining a seed value which is equivalent to a seed value maintained at the source, the seed changing over time, generating a value

based on the seed and based on a value identifying the destination whereby the generated value is different from the seed and the destination's identification value; transmitting the generated value to the source; and **[i.e., referring to Figure 5, as the initial state, a same value I is stored in the first, second and third registers 205, 208 and 212. For the I, a random number shared confidentially by the first and second communication devices (column 11, lines 41-44). Initially, when the transaction IC card 150 is inserted in the card terminal 100 which is equipped with the confirmation IC card 110, the first random number generation means 111 in the confirmation IC card 110 generates random number data R.sub.0, and the first encryption means 112 encrypts the random number data R.sub.0 provided by the first random number generation means 111 by using the first encryption key KE.sub.1 which is stored in advance in the confirmation IC card 110, and sends it to the transaction IC card 150 (column 9, lines 33-42)];**

(2) being authenticated to receive information from the source or send information which will be used by the source, the authentication being dependant upon the source using the seed to extract the destination's identification value and comparing the destination's identification value with the value of a destination known by the source to be authentic **[this limitation is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above].**

f. *Referring to claims 24-29:*

i. These claims have limitations that is similar to those of claims 2-3, thus they are rejected with the same rationale applied against claims 2-3 above.

g. *Referring to claim 30:*

i. This claim has limitations that is similar to those of claim 23, thus it is rejected with the same rationale applied against claim 23 above.

h. *Referring to claim 31:*

i. This claim has limitations that is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

3. Claims 8, 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Ohno (US 5,355,413).

a. *Referring to claim 8:*

i. Takagi teaches:

(1) receiving a first value from the device, the first value being different from an identifier associated with the device; determining the identifier from the value, the value being a function of the identifier and the number of times the device has been authenticated; comparing the identifier determined from the value against a pre-stored identifier; authenticating the device based on the result of the comparison. Maintaining a seed value which is equivalent to a seed value maintained at the source, the seed changing over time, generating a value based on the seed and based on a value identifying the destination whereby the generated value is different from the seed and the destination's identification value; transmitting the generated value to the source; and being authenticated to receive information from the source or send information which will be used by the source, the authentication being dependant upon the source using the seed to extract the destination's identification value and comparing the destination's identification value with the value of a destination known by the source to be authentic **[i.e., in this authentication method, a random number is generated first in the terminal unit, and then the generated random number is sent to the card together with an address specifying the desired authentication code stored in the card. In the IC card, the authentication code corresponding to the given address is obtained. Thereafter, a predetermined processing is performed using the given random number and the obtained authentication code by an encryptor in the IC card itself, and the obtained result of the processing is transmitted to the terminal unit. The terminal unit is also provided with data on the authentication code and the encryptor, like the IC card. Therefore, the terminal unit performs the similar processing to that performed in the IC card on the random number and the authentication code using the encryptor. If the result of the processing performed by the terminal unit coincides with the result of the processing sent from the IC card, the identity of the IC card is established to the terminal unit**

(column 1, lines 20-35). Furthermore, in the authentication method according to the present invention, both the IC card and the terminal unit have a plurality of authentication codes each having a corresponding time data item. When the authentication code selected by one of the IC card and the terminal unit is transmitted to the other, the time data corresponding to the authentication data is transmitted to the other device as a time interval between commands. In the reception side, the selected authentication code is obtained from the time interval between the commands. In both the IC card and the terminal unit, a random number is encrypted according to the encryption algorithm using the authentication code as a key to generate authentication data. The generated authentication data are compared with each other. When they coincide, identity is mutually established (column 2, lines 37-52)].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-7, 17-22, 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takagi et al (US 5,109,152), and further in view of Nakagawa et al (US 5,651,123).

a. *Referring to claim 1:*

i. Takagi teaches:

(1) providing a first device having a first identifier; providing a second device having a second identifier **[i.e., the first communication device is provided with random number generation means and first encryption means, and the second communication device is provided with second encryption means, and therefore a random number flowing from the first communication device to the second communication device is encrypted by the**

first encryption means, and a random number flowing form the second communication device to the first communication device is encrypted by the second encryption means (column 4, lines 46-57)];

(2) the first device sending the first identifier to the second device during a first connection **[i.e., the first processing means which has been granted the information exchange sends the transmission data to the first communication means, and the first communication means 1 uses the random number data provided by the random number generation means to encrypt the entered transmission data and sends it to the card terminal. The encrypted data received by the card terminal is entered to the second communication means, and the second communication means uses the random number data received from the IC card to decrypt the entered encrypted data and enters it to the second processing means. which is the second communication device (column 4, lines 11-23)];**

(3) the second device sending the second identifier to the first device during the first connection **[i.e., the second processing means sends the transmission data to the second communication means, and the second communication means uses the random number data received from the IC card to encrypt the entered data and sends it to the IC card. The encrypted data received by the IC card is entered to the first communication means, and the first communication means uses the random number data provided by the random number generation means to decrypt the entered encrypted data and enters it to the first processing means (column 4, lines 24-36)];**

(4) the first device storing the second identifier and the second device storing the first identifier; when the first and second devices are disconnected and reconnected, the first device sending the first identifier to the second device and the second device sending the second identifier to the first device during the first reconnection, and each device comparing the received identifier against the stored identifier and sending additional information to the other device depending upon the result of the comparison **[i.e., the procedure of creating the identifier described**

above in connection with Figure 6 is completely identical to the procedure of data encryption shown in Figure 5, and it is possible to have the identifier creation process and data encryption process concurrently. Namely, the output of the encryption processes 223-226 in Figure 6 is sent to the second device 202 as an output (encrypted output of transmission data) of the encryption means 204. Specifically, the output of the encryption process 226, i.e., the identifier 231, in Figure 6 is the output of the encryption means 204 for the fixed pattern (P) 215 in Figure 5, and it is stored in the second register 208. Next, the second device 202 uses the second encryption means 211 which performs the same operation as of the first encryption means 204, third register 212 and third exclusive-OR operation means 213 to create comparison data in the same procedure as that of the first device 201 for creating the identifier 231. The comparison data is stored in the third register 212. Finally, the second device 202 uses the comparison means 214 to compare the identifier 231 stored in the second register 208 with the comparison data stored in the third register 212 thereby to verify whether or not the communication data has been tampered (column 12, line 59 through column 13, line 40)];

ii. Although, Takagi does not explicitly mention:

(1) disconnected and reconnected between the first and second devices.

iii. Examiner takes Official Notice that:

(1) the disconnection and reconnection between the first and second devices were well known at the time the invention was made.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include the disconnection and reconnection between the first and second devices. Such an application would have been obvious because Takagi teaches applicability to insert the first device (i.e., IC card) in the card terminal, which is the second device, and because the execution of inserting, un-inserting, and re-inserting the IC card were well known.

b. *Referring to claim 2:*

i. Takagi further teaches:

(1) wherein the step of sending an identifier to the other device includes sending a value that is based on, but not equivalent to, the identifier **[i.e., next, a method of creating the identifier will be explained with reference to Figure 6. Figure 6 is an explanatory diagram showing the procedure of creating the identifier, in which 221 is a plain text block (M.sub.1, M.sub.2, M.sub.3), 215 is a fixed pattern (P) shown in Figure 5, 222 is an initial value I of the first register 205 (column 12, lines 29-34)].**

c. *Referring to claim 3:*

i. Takagi further teaches:

(1) wherein the value sent by the first device is based on the number of times the first device has connected to the second device **[i.e., accordingly, unless the transmission data is altered accidentally or intentionally, the first register 205 and second register 208 always stores the same value. By repeating the process of the leading n-bit data M.sub.1 for the M.sub.2 and M.sub.3 identically, the restored original data are stored sequentially in the restoration block storage means 210 (column 12, lines 15-21)].**

d. *Referring to claim 4:*

i. Takagi further teaches:

(1) wherein the difference between the different values sent each time is pseudo-random **[i.e. the following explains this embodiment with reference to Figure 5. As the initial state, a same value I is stored in the first, second and third registers 205, 208 and 212. For the I, a random number shared confidentially by the first and second communication devices in the first through third embodiments can be used, for example (column 11, lines 40-45)].**

e. *Referring to claim 5:*

i. Takagi further teaches:

(1) wherein the value sent by the first device is determined based on at least one mathematical operation, and at least one of the

purposes of the mathematical operation is to make it difficult to predict the next value to be sent **[i.e., (1) the identifier is dependent on all bits of data of the plain text block. (2) For a plain text m, identifier creation means f, and identifier a=f(m), it is very difficult to obtain x which meets the following: f(m)=f(x) (column12, lines 51-57)]**.

f. *Referring to claims 6 and 7:*

i. These claims have limitations that is similar to those of claim 5, thus they are rejected with the same rationale applied against claim 5 above.

g. *Referring to claim 17:*

i. Takagi teaches:

(1) a pseudo-random number generator using the increment counter value as a seed; memory for storing a value identifying the device; instructions including using the value of the increment counter to extract the value identifying the device from a value transmitted from the device, comparing the identification value with the value stored in memory, and taking the action dependant upon the results of the comparison **[i.e., referring to Figure 9, a card terminal 400 comprises a random number generation means 401 which generates a random number R, a first computation means 402 which performs a functional computation F.sub.1 for first confidential data K.sub.1 and the random number R provided by said random number generation means 401, comparison means 403 which compares data provided by said first computation means 402 and data entered from an IC card 450, first processing means 406 which performs such data processing as data input/output, storing and operation, first encryption means 404 which encrypts the data sent out from said first processing means by using a first encryption key KE.sub.1, second decryption means 405 which decrypts encrypted data entered from the IC card 450 by using a second decryption key KD.sub.2 (column 1, lines 17-31)]**;

ii. However, Takagi does not explicitly mention:

(1) an increment counter associated with a value representing the number of times the system has taken an action in response to a

signal from the device; instructions including using the value of the increment counter to extract the value identifying the device from a value transmitted from the device.

iii. Whereas, Nakagawa teaches:

(1) Figure 1 shows an example of a conventional program execution control device (hereinafter referred to as a "program control unit") for controlling a program execution order in a microprocessor or the like. With reference to FIG. 1, a conventional program control unit includes a program counter (PC) 300, an instruction memory 32, an instruction decoder 34, an incrementer 302 and a selector 304. Instruction memory 32 stores instructions of a program in the order of program addresses. Program addresses are ordinarily set to be incremented one by one. In instruction memory 32, the program addresses are arranged in a continuous memory space whose addresses are incremented one by one. Instruction memory 32 is for reading an instruction word 38 (of m-bit) from an applied n-bit address 310 and applying the word to instruction decoder 34 (column 1, lines 22-36). Nakagawa further discloses with reference to Figure 4, the program control unit of the present embodiment includes an instruction memory 32, an instruction decoder and a pseudo-random number program counter 30. Instruction memory 32 and instruction decoder 34 are the same as those of the conventional device shown in Figure 1, except that a program stored in instruction memory 32 is different from that of Figure 1. The program will be detailed later. An output 38 of instruction memory 32, a control signal 40, a select signal 42 and a jump address 44 output from instruction decoder 34 are also the same as those shown in FIG. 1 and no detailed description thereof will be repeated here **(column 7, lines 12-24).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include a pseudo-random number program counter and an instruction memory (in Takagi) to improve the communication between the two devices.

v. The ordinary skilled person would have been motivated to:

(1) include a pseudo-random number program counter and an instruction memory (in Takagi) to provide program execution control devices for storing instructions in an instruction storage device and designating addresses of the device to read the instructions at high speed in a specific order and apply the same to a program execution device and a method thereof **(column 1, lines 8-12 of Nakagawa).**

h. *Referring to claim 18:*

i. This claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

i. *Referring to claims 19, 20:*

i. Takagi further teaches:

(1) wherein the system is a toy and the device defines functions to be performed by the toy; wherein the toy is a doll **[i.e., the first communication device (e.g., an IC card, toy, games, doll, etc..) is provided with random number generation means and first encryption means, and the second communication device (e.g., a card terminal, PC, host computer, another toy, etc...) is provided with second encryption means, and therefore a random number flowing from the first communication device to the second communication device is encrypted by the first encryption means, and a random number flowing form the second communication device to the first communication device is encrypted by the second encryption means (column 4, lines 46-57)]**.

j. *Referring to claim 21:*

i. This claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

k. *Referring to claim 22:*

i. This claim has limitations that is similar to those of claim 18, thus it is rejected with the same rationale applied against claim 18 above.

l. *Referring to claim 32:*

i. This claim has limitations that is similar to those of claim 18, thus it is rejected with the same rationale applied against claim 18 above.

m. *Referring to claim 33:*

i. Takagi further teaches:

(1) wherein the second device further comprises a checksum algorithm providing a value indicative of whether the prestored value was erased **[i.e., the procedure of verifying the identifier will be described with reference to Figure 5. First, a processing means (not shown) of the second device 202 replaces the last n-bit data out of the data stored in the restoration block storage means 210 with the fixed pattern 216. In case communication has taken place normally, the original data to be replaced (that is "the prestored value was erased") is equal to the fixed pattern 216 (column 13, lines 3-7)].**

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kikinis (US 5, 746, 602) discloses an interactive system for teaching, entertaining, and habituating a child utilizes an interactive entity such as a doll, the doll having a microphone, a speaker, and control circuitry adapted for driving the speaker and microphone and a bidirectional communication link to a personal computer (PC) (see abstract).

b. Gabai et al (US 6, 075, 195) discloses Apparatus for a wireless computer controlled toy system is disclosed, the apparatus including a computer system operative to transmit a first transmission via a first wireless transmitter and at least one toy including a first wireless receiver, the toy receiving the first transmission via the first wireless receiver and operative to carry out at least one action based on said first transmission (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TC 2100 will be moved to Carlyle in October 2004, the new telephone number for TC 2100 receptionist is 571-272-2100. In October 2004, any inquiry concerning this communication should be directed to Thanhnga (Tanya) Truong whose new telephone number is 571-272-3858, and the examiner's supervisor, Kim Vu can be reached at 571-272-3859.

AU 2135

TBT

October 15, 2004